关于 m 序列的自旋转缩减序列 [1]

胡予濮 肖国镇

(西安电子科技大学应用数学系 西安 710071)

摘 要 本文介绍 m 序列的自旋转缩减序列；讨论了它的整齐的代数性质和良好的密码学性质．作为实用，本文提出一种具有少量存储和判别的旋转缩减序列链接方案．

关键词 流密码，m 序列，自旋转缩减序列

中图号 TN918.1

1 引言和定义

众所周知，高质量的流密码的设计应满足：(1) 良好的各种伪随机特性；(2) 极大的线性复杂度；(3) 充分隐蔽驱动序列 [1]．目前通用的设计方法是非线性前馈和变间隔采样 (即钟控)[2]．Coppersmith 等人提出一种新的伪随机序列发生器，称为缩减发生器 [3]，可直接作为流密码使用．缩减发生器概念简洁，只有两个线性反馈移位寄存器组成，因此颇引人注意．有人猜想如此简单的构造也许不够安全，但至今仍无成功的分析攻击文章发表．Willi Meier 将缩减发生器更减化为自缩发生器 [4]，只用一个线性移位寄存器得到一个隔位受控输出序列．本文提出的自旋转缩减序列是文献 [3] 中缩减序列的特例，是文献 [4] 中的自缩发生器的推广．与文献 [3] 相比，自旋转缩减序列具有更为清晰的代数结构和密码学性质；与文献 [4] 相比，自旋转缩减发生器具有更强的安全性．本文讨论了自旋转缩减序列的整齐的代数性质，它的周期和线性复杂度，并提出一种只需少量存储和判别的自旋转缩减序列链接方案．

设 $a=a_0a_1a_2\cdots$ 是二元 m 序列，其周期为 2^n-1．$a^{(k)}=a_0^{(k)}a_1^{(k)}a_2^{(k)}\cdots=a_ka_{k+1}a_{k+2}\cdots$ 是序列 a 的 k 步平移等价序列，其中 k 为任意整数．

对于输入序列 a 和 $a^{(k)}$，若 $a_i=1$ 则输出 $a_i^{(k)}$；若 $a_i=0$ 则放弃输出．如此得到输出序列 $b^{(k)}=b_0^{(k)}b_1^{(k)}b_2^{(k)}\cdots$．称 $b^{(k)}$ 为 a 的自旋转缩减序列．

2 代数结构

显然 $b^{(0)}=1=111\cdots$．自旋转缩减序列 $b^{(k)}$，$k=0,1,2,\cdots,2^n-2$，再添上序列 $0=000\cdots$，构成了序列族 B．

定理 1 (1) 序列族 B 按逐位模 2 加法 $\oplus$ 构成群；(2) 序列族 B 构成 $[\mathrm{GF}(2)]^{2^n-1}$ 上的 n 维线性子空间．

证 对于 $k,l=0,1,2,\cdots,2^n-2$，

$$a^{(k)}\oplus a^{(l)}=\begin{cases}0, & \text{当}k=l;\\ a^{(m)},\text{其中}m\text{是}0\sim 2^n-2\text{中的某个整数}, & \text{当}k\neq l;\end{cases}$$

[1] 1995-12-25 收到，1997-03-10 定稿

故有

$$b^{(k)} \oplus b^{(k)} = \begin{cases} 0, & \text{当} k = l; \\ b^{(0)} = 1, & \text{当} a^{(k)} \oplus a^{(l)} = a, k \neq l; \\ b^{(m)}, & \text{当} a^{(k)} \oplus a^{(l)} = a^{(m)} \neq a, k \neq l, \end{cases}$$

$b^{(k)} \oplus 0 = b^{(k)}$ 。 (1) 得证。

显然序列族 B 是 $[\mathrm{GF}(2)]^{2^{n-1}}$ 上的线性子空间。又知当 $k \neq l$ 时 $b^{(k)} \neq b^{(l)}$, 故 B 有 2^n 个不同序列，即 B 的维数为 n 。 证毕

推论 1 对于每个 $b^{(k)}$, $k \neq 0$, 2^{n-1} 是 $b^{(k)}$ 的一个周期，且 $b^{(k)}$ 在周期内是 0-1 对称分布的。

证 由 m 序列的自相关性质即得。 证毕

推论 2 对于 $k, l = 0, 1, 2, \cdots, 2^n - 2$, 记 $\mathrm{cov}(b^{(k)}, b^{(l)}) \triangleq \frac{1}{N} \sum_{i=0}^{N-1} (1 - 2b_i^{(k)}) \cdot (1 - 2b_i^{(l)})$, 其中 $N = 2^{n-1}$, 则有

$$\mathrm{cov}(b^{(k)}, b^{(l)}) = \begin{cases} 1, & \text{当} k = l; \\ -1, & \text{当} k \neq l, a^{(k)} \oplus a^{(l)} = a; \\ 0, & \text{当} k \neq l, a^{(k)} \oplus a^{(l)} = a^{(m)} \neq a. \end{cases}$$

证 由定理 1 的证明即得。 证毕

当 $\mathrm{cov}(b^{(k)}, b^{(l)}) = -1$ 时，称 $b^{(k)}$ 与 $b^{(l)}$ 互为补序列，记为 $b^{(k)} = \overline{b^{(l)}}$ 或 $b^{(l)} = \overline{b^{(k)}}$ 。此时 $b^{(k)} \oplus \overline{b^{(k)}} = 1$, 且 $b^{(k)}$ 与 $\overline{b^{(k)}}$ 相互唯一。

此类自旋转缩减序列可以再次进行自旋转缩减。取固定的 k_0, $0 < k_0 \leq 2^n - 2$; 再取 k 为整数。对于输入序列 $b^{(k_0)}, b^{(k)}$, 若 $b_i^{(k_0)} = 1$, 则输出 $b_i^{(k)}$; 若 $b_i^{(k_0)} = 0$ ，则放弃输出。如此得到输出序列 $c^{(k)} = c_0^{(k)} c_1^{(k)} c_2^{(k)} \cdots$ 。称 $c^{(k)}$ 为 $b^{(k_0)}$ 的二次自旋转缩减序列。二次自旋转缩减序列 $c^{(k)}$, $k = 0, 1, 2, \cdots, 2^n - 2$, 构成序列族 C 。

定理 2 (1) 序列族 C 按逐位模 2 加法 $\oplus$ 构成群。 (2)C 是 $[\mathrm{GF}(2)]^{2^{n-2}}$ 上的 $n-1$ 维线性子空间。

证 略。

3 最小周期和线性复杂度

关于自旋转缩减序列的最小周期 p, 我们已知道 $p | 2^{n-1}$ 。并且有以下两个定理。

定理 3 序列族 B 中，至少有一半的序列 (2^{n-1} 个) 其最小周期为 $p = 2^{n-1}$ 。

证 设 B 中最小周期 $p < 2^{n-1}$ 的序列的全体构成序列族 B_0 。易证 B_0 是 B 的子群和线性子空间。于是有 $|B_0| = 2^m$, $m \leq n$ 。再由 m 序列的性质易知： $b^{(1)}$ 在连续的 2^{n-1} 位中，最长的 1-游程，长度为 $n-1$, 且只有一个，故 $b^{(1)}$ 的最小周期为 2^{n-1} 。所以 $|B_0| = 2^m$, $m < n$ 。

证毕

定理 4 序列族 B 中恰有一对 (两个) 序列是最小周期 $p = 2$ 的。

证 设 a 的最小生成多项式为

$$f(x) = 1 + u_1 x + u_2 x^2 + \cdots + u_n x^n, \qquad u_n = 1. \tag{1}$$

由 a 的初始状态 $(a_{-1},a_{-2},\cdots,a_{-n})$ 生成 a:

$$\left.\begin{aligned} a_0 &= u_1a_{-1}+u_2a_{-2}+\cdots+u_na_{-n},\\ a_m &= v_{m1}a_{-1}+v_{m2}a_{-2}+\cdots+v_{mn}a_{-n}. \end{aligned}\right\} \tag{2}$$

由 (1),(2) 两式即得

$$\begin{aligned} a_{m+1} &= v_{m1}a_0+v_{m2}a_{-1}+\cdots+v_{mn}a_{-n+1}\\ &= v_{m1}(u_1a_{-1}+u_2a_{-2}+\cdots+u_na_{-n})+v_{m2}a_{-1}+\cdots+v_{mn}a_{-n+1}\\ &= v_{m+1,1}a_{-1}+v_{m+1,2}a_{-2}+\cdots+v_{m+1,n}a_{-n}. \end{aligned} \tag{3}$$

为简单起见，不妨设 $a_{-1}=a_{-2}=\cdots=a_{-n}=1$，则有：(1) $(v_{m1},v_{m2},\cdots,v_{mn})$ 中有奇数个 1 时，$a_m=1$；否则 $a_m=0$；(2) $(u_1,u_2,\cdots,u_n)$ 中必有偶数个 1，即 $a_0=0$；(3)$a_{m+1}\neq a_m$ 的充要条件是 $v_{m1}=1$。

设 $a'=a'_0a'_1a'_2\cdots$ 是 a 的平移等价序列，其初始状态为 $(a'_{-1},a'_{-2},\cdots,a'_{-n})=(0,1,0,1,\cdots)$ 或 $(1,0,1,0,\cdots)$。

以下分两种情形讨论：

(1) 当 $a_m=a_{m+1}=1$ 时，要证明 $a'_{m+1}\neq a'_m$。由于 $(v_{m1},v_{m2},\cdots,v_{mn})$ 中有奇数个 1，且 $v_{m1}=0$，故 $(v_{m+1,1},v_{m+1,2},\cdots,v_{m+1,n})=(v_{m2},v_{m3},\cdots,v_{mn},0)$。

$$\left.\begin{aligned} a'_m &= (v_{m1},\cdots,v_{mn})\cdot(a'_{-1},a'_{-2},\cdots,a'_{-n})^\tau,\\ a'_{m+1} &= (v_{m2},\cdots,v_{mn},0)\cdot(a'_{-1},a'_{-2},\cdots,a'_{-n})^\tau, \end{aligned}\right\}$$

故由此得 $a'_{m+1}\neq a'_m$。

(2) 当 $a_m=1\neq a_{m+1}=a_{m+2}=\cdots=a_{m+l}=0\neq a_{m+l+1}=1$ 时，要证明 $a'_{m+l+1}\neq a'_m$。

设 $a'_0=(u_1,u_2,\cdots,u_n)\cdot(a'_{-1},a'_{-2},\cdots,a'_{-n})^\tau=a'_0$，若 $(a'_{-1},a'_{-2},\cdots,a'_{-n})=(0,1,0,1,\cdots)$，则

$$\begin{aligned} a'_{m+1} &= a'_0+a'_m=a'_{m+2}=\cdots=a'_{m+l},\\ a'_{m+l+1} &= a'_{m+l}+1+a'_0=a'_m+a'_0+1+a'_0=a'_m+1\neq a'_m; \end{aligned}$$

若 $(a'_{-1},a'_{-2},\cdots,a'_{-n})=(1,0,1,0,\cdots)$，则

$$\begin{aligned} a'_{m+1} &= a'_0+a'_m+1=a'_{m+2}=\cdots=a'_{m+l},\\ a'_{m+l+1} &= a'_{m+l}+a'_0=a'_m+a'_0+1+a'_0=a'_m+1\neq a'_m; \end{aligned}$$

综上所述可知，由 a 和 a' 产生的自旋转缩减序列是最小周期 $p=2$ 的，且这样的 a' 仅有两个。　　证毕

结论远不止于此。有理由相信：对于 m 序列 a，任取 $b\in B$，$b=b_0b_1b_2\cdots$，则以极大的概率使 b 的最小周期 $p=2^{n-1}$，理由如下：

(1) 随机取一个长度为 2^{n-1} 且 0-1 对称分布的序列，则其最小周期 $p<2^{n-1}$ 的概率为 $P=C^{2^{n-2}}_{2^{n-2}}/C^{2^{n-2}}_{2^{n-1}}$，$2^{5-2n}\leq P\leq 2^{6-2n}$。

(2)b 的最小周期 $p<2^{n-1}$ 等价于一个“苛刻”的条件：对于所有的 j，$\sum_{i=j+1}^{j+2^{n-2}}b_i=2^{n-3}$。

(3) 对于小 n 的试验结果

注意到 m 序列的互反特性和等价性，由穷举得到以下结论．设 $n=3,4,5,6$．每一个 n 级 m 序列 a，其 2^n-2 个自旋转缩减序列中，有 2^n-4 个序列是最小周期为 2^{n-1} 的．

试验还表明，一般的生成多项式甚至既约多项式都不具有以上的结论，因此猜测以上结论是由本原多项式的特性所致，故有

猜想 对每一个 n 级 m 序列 a，其对应的序列族 B 中，有 2 个序列最小周期为 1，有 2 个序列最小周期为 2，其余 2^n-4 个序列均是最小周期为 2^{n-1} 的 ($n\le 6$ 时已由试验所证明)．

定理 5 [1,2] 若序列 $b=b_0b_1b_2\cdots$ 的最小周期为 $p=2^k$，$k\le n-1$，则其线性复杂度 $L>2^{k-1}$．

4 生成的多重性

设由 m 序列 a 和它的 k 步平移等价序列 $a^{(k)}$ 生成了自旋转缩减序列 $b^{(k)}$，作为序列密码的安全性考虑，一个自然关心的问题是：$b^{(k)}$ 能否由 a 的另一对平移等价序列 $a^{(l_1)}$ 和 $a^{(l_2)}$ 共同生成？

以下将序列族 B 中的所有序列均作 k 步平移得到序列族 $B^{(k)}$，于是得到 2^{n-1} 个序列族 $B,B^{(1)},B^{(2)},\cdots,B^{2^{n-1}-1}$．

定理 6 若 $n\le 2^{n-2}$，则 $B^{(1)}\ne B$．

证 不妨设 a 的前 n bit 均为 1．观察 B 中的 2^n 个序列，易知它们的前 n bit 是互不相同的，且取遍 $[\mathrm{GF}(2)]^n$；$\forall b=b_0b_1b_2\cdots\in B$，由于 a 是线性移位序列，故 $b_n=u_1b_{n-1}+u_2b_{n-2}+\cdots+u_nb_0$，且 $(u_1,u_2,\cdots,u_n)$ 与 $b\in B$ 无关．

若 $B^{(1)}=B$，则易见 $B^{(1)}=B^{(2)}=\cdots=B^{(2^{n-1}-1)}=B$．即 $\forall b\in B$，b 的任一个平移等价序列也属于 B．设 $b=b_0b_1b_2\cdots\in B$，b 的 k 步平移等价序列为 $b'=b_kb_{k+1}b_{k+2}\cdots\in B$，于是有 $b_{k+n}=u_1b_{k+n-1}+u_2b_{k+n-2}+\cdots+u_nb_k$．由 k 的任意性知 b 是 n 级线性移位序列，再由 $b\in B$ 的任意性知 B 中所有序列的线性复杂度 $L\le n$．但由定理 3 和定理 5，B 中确有序列 b 其线性复杂度 $L>2^{n-2}\ge n$．矛盾． 证毕

推论 1 若 $n\le 2^{n-2}$，则对奇数 k，$B^{(k)}\ne B$．

证 若 $B^{(k)}=B$，则 $B^{(lk)}=B$，$l=1,2,\cdots$．存在 l_0 使 $l_0k=1[\mathrm{mod}(2^{n-1})]$，故 $B^{(l_0k)}=B^{(1)}=B$． 证毕

推论 2 若 $B^{(k)}\ne B$，则 $|B^{(k)}\cap B|\le 2^{n-1}$．

试验表明：$B,B^{(1)},B^{(2)},\cdots,B^{(2^{n-1}-1)}$ 之间的重合率极小．

5 链接方案

利用少量的存储和判别，可将 B 中的序列链接成为周期和线性复杂度都更大的序列．一种链接方案如下．

计算存储单元 两个 n 级线性移存器 LFSR_1 和 LFSR_2；一个 n bit 存储器 R；一个 $n-1$ 位计数器 M．

密钥 n 级本原多项式 $f(x)$；初始增量 u，其中 u 是正整数，且 $\gcd(u,2^n-1)=1$；数 α．

程序

(1) 置 $M=0$，$\mathrm{LFSR}_1=\alpha u[\mathrm{mod}(2^n-1)]$；

(2) 置 $\mathrm{LFSR}_2=\mathrm{LFSR}_1+u[\mathrm{mod}(2^n-1)]$；$R=\mathrm{LFSR}_2$；

(3) 同步驱动，由 LFSR_1 的输出序列 a 和 LFSR_2 的输出序列 $a^{(k)}$，得自旋转缩减序列 $b^{(k)}$ 的 2^{n-1} 位；

(4) 若 $\mathrm{LFSR}_2 = R$, 则置 $M = M + 1$;

(5) 若 $M \neq 2^{n-1} - 1$, 则置 $\mathrm{LFSR}_2 = \mathrm{LFSR}_2 + u$, 则转 (3); 若 $M = 2^{n-1} - 1$, 转 (1) .

6 结束语

直观看来，自旋转缩减序列是一种非布尔生成的序列，它对原驱动序列的泄露极不规则，因而有很强的隐蔽性. 自旋转缩减序列的游程分布在理论上是未知的，虽然作者对 $n \leq 6$ 时的所有自旋转缩减序列的观察说明它们大都有良好的游程分布.

参 考 文 献

[1] Rueppel R. Analysis and Design of Stream Ciphers, Berlin: Springer-Verlag, 1986, 5–16.

[2] 丁存生，肖国镇. 流密码学及其应用. 北京：国防工业出版社， 1994, 130–159, 181–204.

[3] Coppersmith D, Krawcyk H. The shrinking generator, Crypto'93, Springer-Verlag, Berlin, Heidelberg, New York: 22–39.

[4] Meier W, Staffelbach O. Self-shrinking generator, Eurocrypt'94, Peruginna: 1994.

[5] 陈爱明，等. 计算机的安全与保密. 北京：电子工业出版社， 1992, 39–78.

ON SELF-ROTATION-SHRINKING-SERIES OF m-SERIES

Hu Yupu　　Xiao Guozhen

(*Department of Applied Mathematics, Xidian University, Xi'an* 710071)

Abstract　In this article, self-rotation-shrinking-series of m-series are introduced; their elegant algebraic structure and nice cryptic features are discussed. For practical application, a linking scheme with a little stores and judgements is proposed.

Key words　Stream cipher, m-series, Self-rotation-shrinking-series

胡予濮：　男， 1955 年生，副教授，从事概率统计方面的科研教学工作.

肖国镇：　男， 1933 年生，教授，博士生导师，从事信息安全保密领域的科研教学工作.